DFW

TO: UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Brian McKeon
Application/Control Number:	10/767,529
Original Filing Date:	29/Jan/2004
Art Unit:	2139
Examiner:	TABOR, AMARE F
For:	Regulated Issuance of Digital Certificates
Date:	26/Nov/2008

Dear Sir,
I noted in your PAIR system that my response of August this year filed in response to the Office Action dated 29/May/2008 has been received by your office but it does not seem to have been recognized as a response. I did contact the examiner of this application and he said that the response had not been forwarded to him. He suggested that the response may have been non-conforming but I have had no notice of this.

I am therefore assuming that the response may have been non-conforming and I am therefore resubmitting the same information in a more explicit format. I have also removed the figures that were in my previous response in case they were a problem. I have replaced these with a text response.

I hope that the attached discussion addresses your questions. If there are any of the above points that could be clarified via email or phone I can be contacted at brian.mckeon@sentrypm.com or on +61-413-401-555.

Yours Sincerely

Brian McKeon

Attachments:
1. Discussion

Claims 1, 3, 4 and 6-8 of 10/767,529 were rejected under 35 U.S.C. 102(e) as being anticipated by "Aull" (US 7,047,409 B1).

The examiner has noted that Aull cites *"an automated registration arrangement...can be accessed only via the associated pedigree certificate,... if a user accesses one of the ...registration web pages, the* ***user must be employing the special hardware*** *of the corresponding category since only that category of hardware possesses the requisite pedigree certificate and associated private key. Thus the* ***user can be issued a digital certificate*** *having a level of trust commensurate with the pedigree certificate of the special hardware of the user."*

Considering the identified aspects.

Both Aull and 10/767,529 describe the use of modules or special hardware that is trusted by the registration or certification authority.

Aull describes a method whereby a hardware token is associated with **an end-user** and where the token is known to be trusted via a pedigree certificate and associated trust mechanism and **the trusted hardware token can then be issued with an individual certificate** associated with the holder of the hardware token. The token then becomes personalized to a user.

10/767,529 associates hardware tokens with an intermediate authority, not an end-user. The hardware tokens are **not designed or intended to be stores of user tokens**. The **hardware token issues certificates to end-users**. This is clearly distinct to Aull where the hardware token is the end-recipient of the user certificate.

Aull describes a scheme where the hardware token requests personalized certificates from the registration (certificate) authority. 10/767,529 describes a scheme where the hardware token provides a service to such requests so is at a different point in the certificate issuance scheme.

In essence the following shows the issuance of individual certificates in the system described by Aull.

Certificate Authority (CA) **issues** individual Certificates **targeted to** Hardware User token (User keys and Certificates).

The following shows the issuance of individual certificates in 10/767,529.

Certificate Authority (CA) **issues** periodic tickets **targeted to** Hardware token and this token **issues** User keys and Certificates.

The invention disclosed in application 10/767,529 uses hardware tokens, not as a certificate and key store for end-users but as an intermediate Certificate Authority that can be securely regulated by the parent CA.

The intermediate, sub-issuance CA handles the routine requests from users for certificates. The main CA needs only deal with periodic requests for tickets, significantly lowering overheads on the main CA. The requirement for the hardware token at the sub-issuance CA is so that the main CA can be confident that the certificates issued by the sub-issuance CA are regulated. That is, the number of certificates issued are regulated, and the format of the certificates is also regulated.

The hardware token for the sub-issuance CA also securely stores the sub-issuance keys of the CA. These are issuance keys that are for certification of user keys in the user tokens. Private user keys are not stored in the hardware token of the sub-issuance CA.

Application 10/767,529 is not concerned with the hardware format of the end-user key and certificate storage. The user may store their private key and certificate in a software format such as used by many PC operating systems or the user may use a hardware device such as a USB token, smartcard etc, depending on the security policy of their situation.

Please advise if the above information is sufficient to allow reconsideration and withdrawal of the rejection of claim 1 of application 10/767,529. If this is the case then this should allow the remaining claims which are dependent on claim 1.

I hope that the attached discussion addresses your questions. If there are any of the above points that could be clarified via email or phone I can be contacted at brian.mckeon@sentrypm.com or on +61-413-401-555.

Yours Sincerely

Brian McKeon